Network Security and Vulnerability Assessment with Nmap

By: Michael Emil Santos

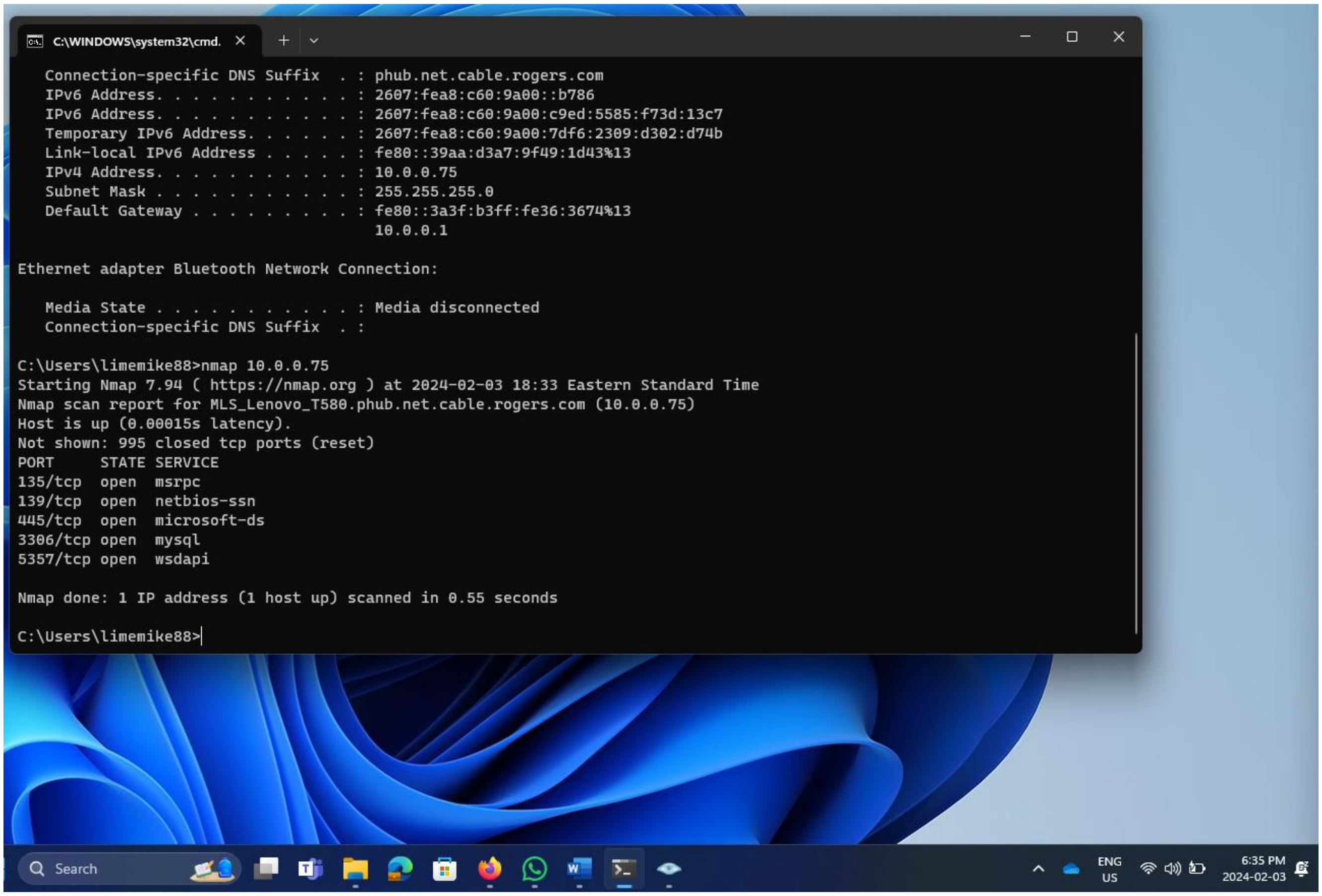
Introduction:

- This project demonstrates the use of Nmap, a versatile network scanning tool, to perform a detailed security assessment on a network. By leveraging Nmap's scanning capabilities, I have identified active hosts, open ports, running services, and potential vulnerabilities, showcasing skills in network security analysis and proactive risk management.

Project Objectives and Methodology:

1. Port and Service Scanning: To identify open ports and active services on network devices. Using basic Nmap commands, I scanned specific IP addresses to detect open ports and the services running on them, helping to understand the network's security profile and accessible points.

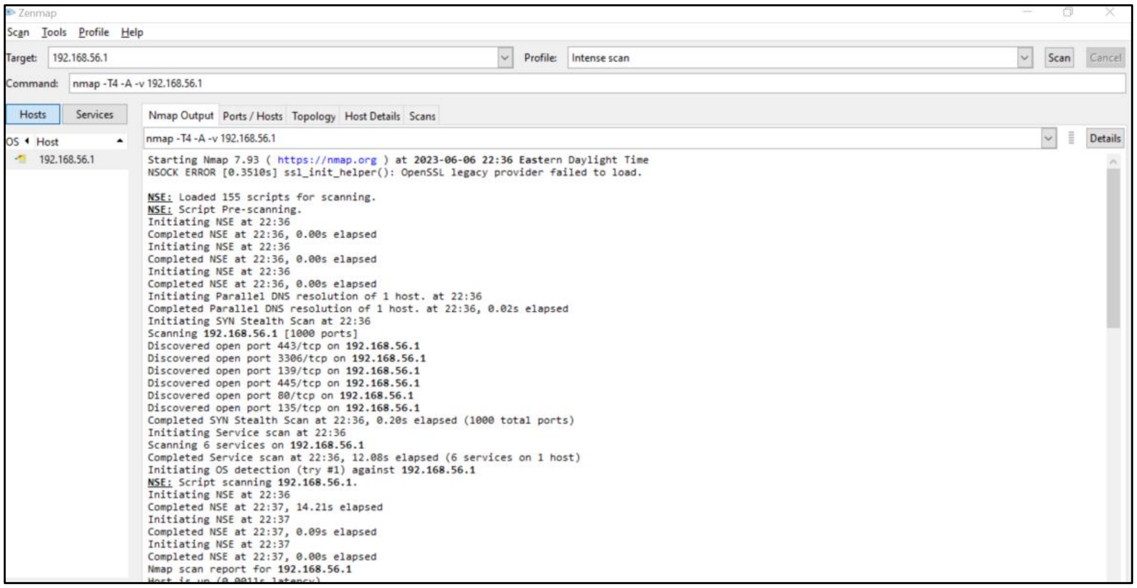
Performing nmap scan using command prompt:



```
   Connection-specific DNS Suffix  . : phub.net.cable.rogers.com
   IPv6 Address. . . . . . . . . . . : 2607:fea8:c60:9a00::b786
   IPv6 Address. . . . . . . . . . . : 2607:fea8:c60:9a00:c9ed:5585:f73d:13c7
   Temporary IPv6 Address. . . . . . : 2607:fea8:c60:9a00:7df6:2309:d302:d74b
   Link-local IPv6 Address . . . . . : fe80::39aa:d3a7:9f49:1d43%13
   IPv4 Address. . . . . . . . . . . : 10.0.0.75
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::3a3f:b3ff:fe36:3674%13
                                       10.0.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\limemike88>nmap 10.0.0.75
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 18:33 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00015s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

C:\Users\limemike88>
```

Another way is to open the terminal, we will see a default command.

nmap -T4 -A -v 192.168.56.1:   scan all information this IP address

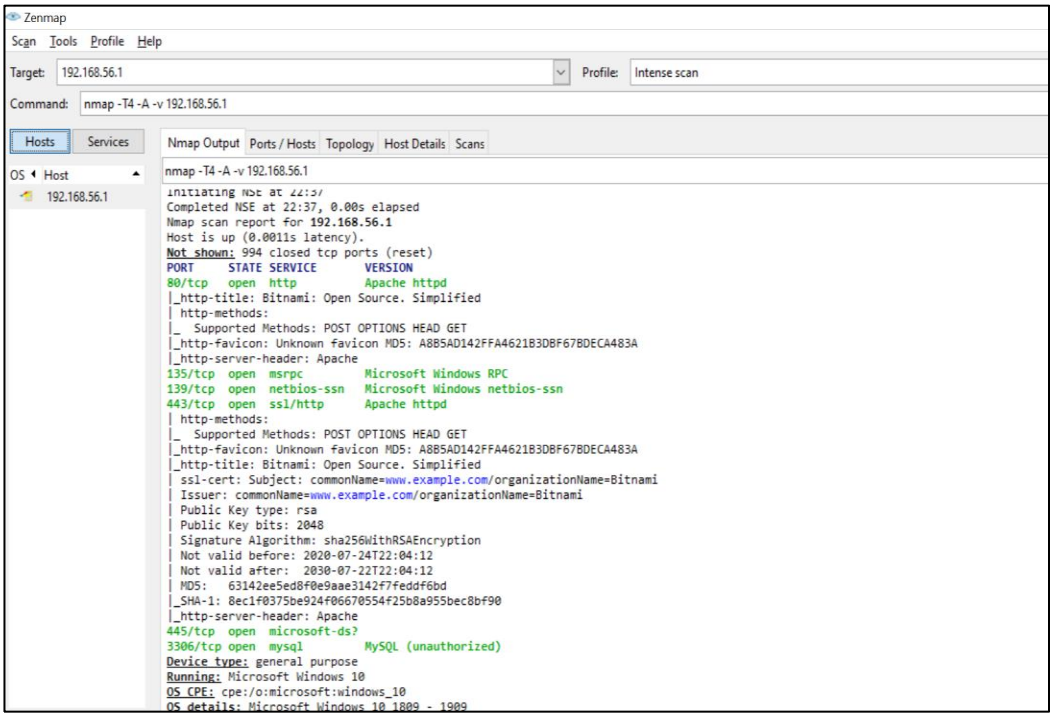


Target: 192.168.56.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.56.1

```
nmap -T4 -A -v 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-06 22:36 Eastern Daylight Time
NSOCK ERROR [0.3510s] ssl_init_helper(): OpenSSL legacy provider failed to load.

NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:36
Completed NSE at 22:36, 0.00s elapsed
Initiating NSE at 22:36
Completed NSE at 22:36, 0.00s elapsed
Initiating NSE at 22:36
Completed NSE at 22:36, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:36
Completed Parallel DNS resolution of 1 host. at 22:36, 0.02s elapsed
Initiating SYN Stealth Scan at 22:36
Scanning 192.168.56.1 [1000 ports]
Discovered open port 443/tcp on 192.168.56.1
Discovered open port 3306/tcp on 192.168.56.1
Discovered open port 139/tcp on 192.168.56.1
Discovered open port 445/tcp on 192.168.56.1
Discovered open port 80/tcp on 192.168.56.1
Discovered open port 135/tcp on 192.168.56.1
Completed SYN Stealth Scan at 22:36, 0.20s elapsed (1000 total ports)
Initiating Service scan at 22:36
Scanning 6 services on 192.168.56.1
Completed Service scan at 22:36, 12.08s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.1
NSE: Script scanning 192.168.56.1.
Initiating NSE at 22:36
Completed NSE at 22:37, 14.21s elapsed
Initiating NSE at 22:37
Completed NSE at 22:37, 0.09s elapsed
Initiating NSE at 22:37
Completed NSE at 22:37, 0.00s elapsed
Nmap scan report for 192.168.56.1
Host is up (0.0011s latency).
```



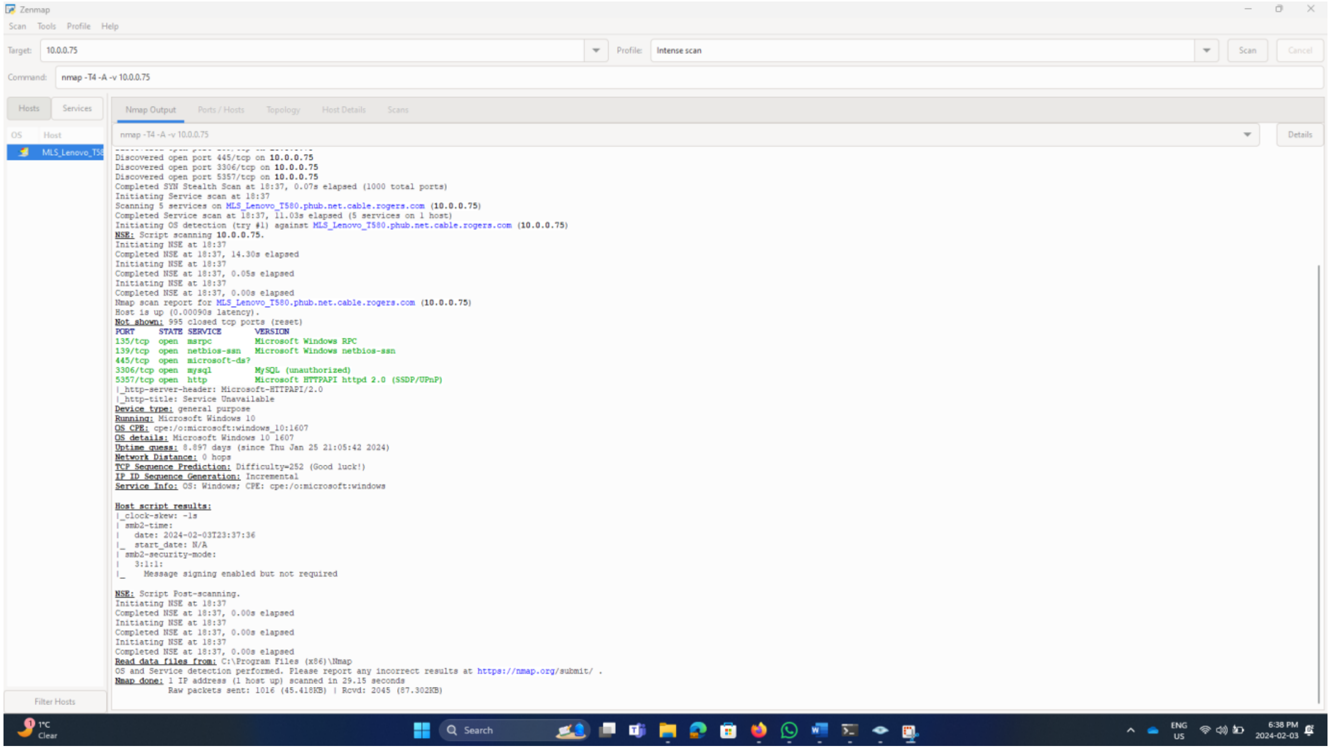
Target: 192.168.56.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.56.1

```
nmap -T4 -A -v 192.168.56.1
Initiating NSE at 22:37
Completed NSE at 22:37, 0.00s elapsed
Nmap scan report for 192.168.56.1
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd
|_http-title: Bitnami: Open Source. Simplified
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-favicon: Unknown favicon MD5: A8B5AD142FFA4621B3DBF67BDECA483A
|_http-server-header: Apache
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-favicon: Unknown favicon MD5: A8B5AD142FFA4621B3DBF67BDECA483A
|_http-title: Bitnami: Open Source. Simplified
| ssl-cert: Subject: commonName=www.example.com/organizationName=Bitnami
| Issuer: commonName=www.example.com/organizationName=Bitnami
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-07-24T22:04:12
| Not valid after:  2030-07-22T22:04:12
| MD5:   63142ee5ed8f0e9aae3142f7feddf6bd
|_SHA-1: 8ec1f0375be924f06670554f25b8a955bec8bf90
|_http-server-header: Apache
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
```

Performing nmap scan using Zenmap GUI:



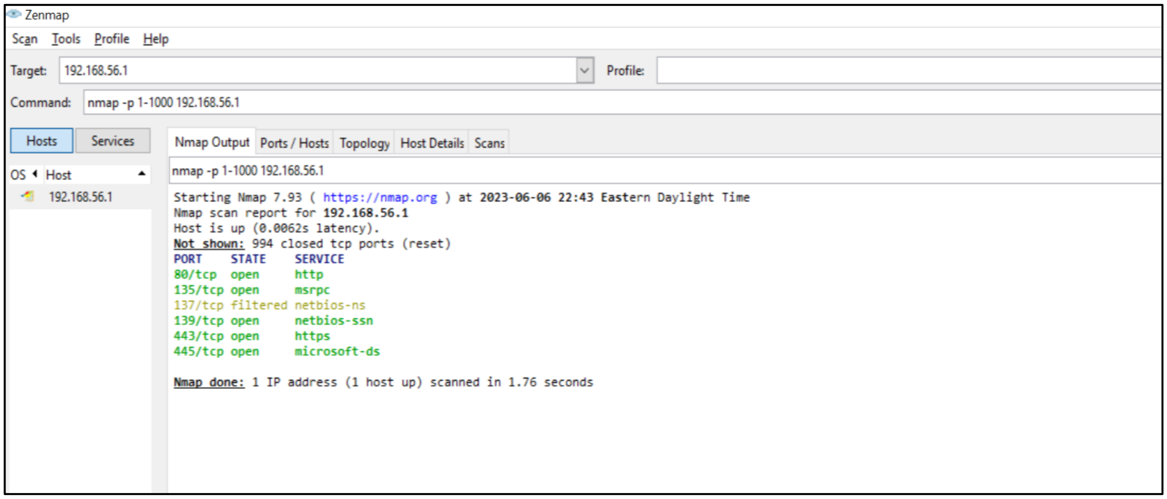
Target: 10.0.0.75

Profile: Intense scan

Command: nmap -T4 -A -v 10.0.0.75

```
nmap -T4 -A -v 10.0.0.75
Discovered open port 445/tcp on 10.0.0.75
Discovered open port 3306/tcp on 10.0.0.75
Discovered open port 5357/tcp on 10.0.0.75
Completed SYN Stealth Scan at 18:37, 0.07s elapsed (1000 total ports)
Initiating Service scan at 18:37
Scanning 5 services on MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Completed Service scan at 18:37, 11.03s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
NSE: Script scanning 10.0.0.75.
Initiating NSE at 18:37
Completed NSE at 18:37, 14.30s elapsed
Initiating NSE at 18:37
Completed NSE at 18:37, 0.05s elapsed
Initiating NSE at 18:37
Completed NSE at 18:37, 0.00s elapsed
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00090s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Uptime guess: 8.897 days (since Thu Jan 25 21:05:42 2024)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -1s
| smb2-time:
|   date: 2024-02-03T23:37:36
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 18:37
Completed NSE at 18:37, 0.00s elapsed
Initiating NSE at 18:37
Completed NSE at 18:37, 0.00s elapsed
Initiating NSE at 18:37
Completed NSE at 18:37, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.15 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2045 (87.302KB)
```

Nmap offers a variety of scan options that can be used to customize the scan to meet your needs. For example, you can use the "-sS" option to perform a stealth scan, which attempts to avoid detection by firewalls and intrusion detection systems. You can also use the "-p" option to specify a range of ports to scan.



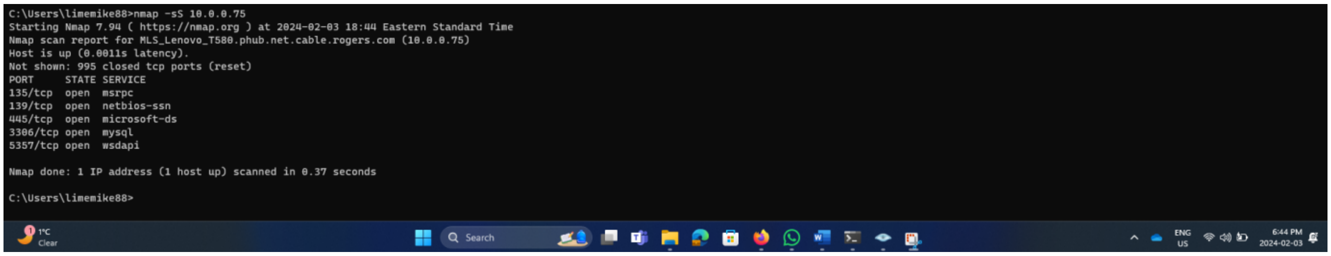
Target: 192.168.56.1

Profile:

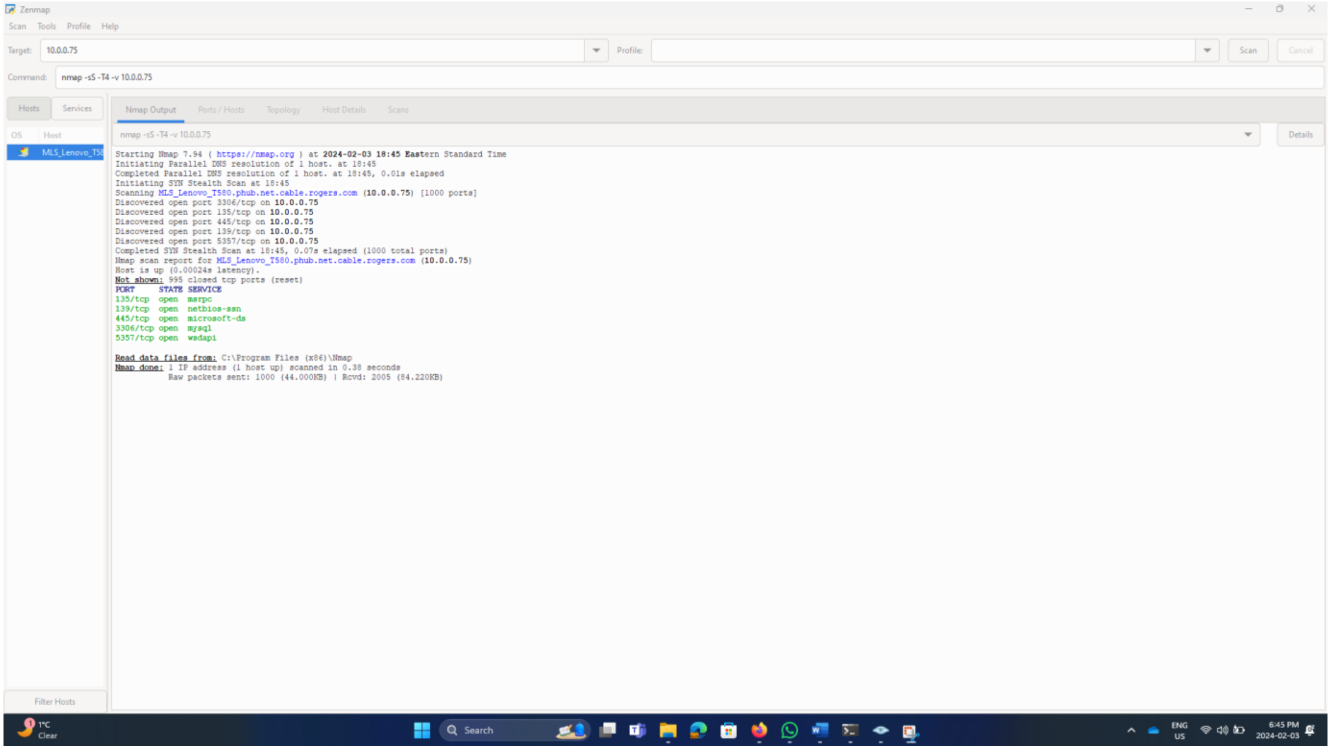
Command: nmap -p 1-1000 192.168.56.1

```
nmap -p 1-1000 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-06 22:43 Eastern Daylight Time
Nmap scan report for 192.168.56.1
Host is up (0.0062s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE    SERVICE
80/tcp   open     http
135/tcp  open     msrpc
137/tcp  filtered netbios-ns
139/tcp  open     netbios-ssn
443/tcp  open     https
445/tcp  open     microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```

Performing nmap scan using "-sS" function in command prompt and Zenmap Gui:



```
C:\Users\limemike88>nmap -sS 10.0.0.75
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 18:44 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.0011s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds

C:\Users\limemike88>
```



Target: 10.0.0.75

Command: nmap -sS -T4 -v 10.0.0.75

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 18:45 Eastern Standard Time
Initiating Parallel DNS resolution of 1 host. at 18:45
Completed Parallel DNS resolution of 1 host. at 18:45, 0.01s elapsed
Initiating SYN Stealth Scan at 18:45
Scanning MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75) [1000 ports]
Discovered open port 3306/tcp on 10.0.0.75
Discovered open port 135/tcp on 10.0.0.75
Discovered open port 445/tcp on 10.0.0.75
Discovered open port 139/tcp on 10.0.0.75
Discovered open port 5357/tcp on 10.0.0.75
Completed SYN Stealth Scan at 18:45, 0.07s elapsed (1000 total ports)
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00024s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
           Raw packets sent: 1000 (44.000KB) | Rcvd: 2005 (84.220KB)
```

Explanation:

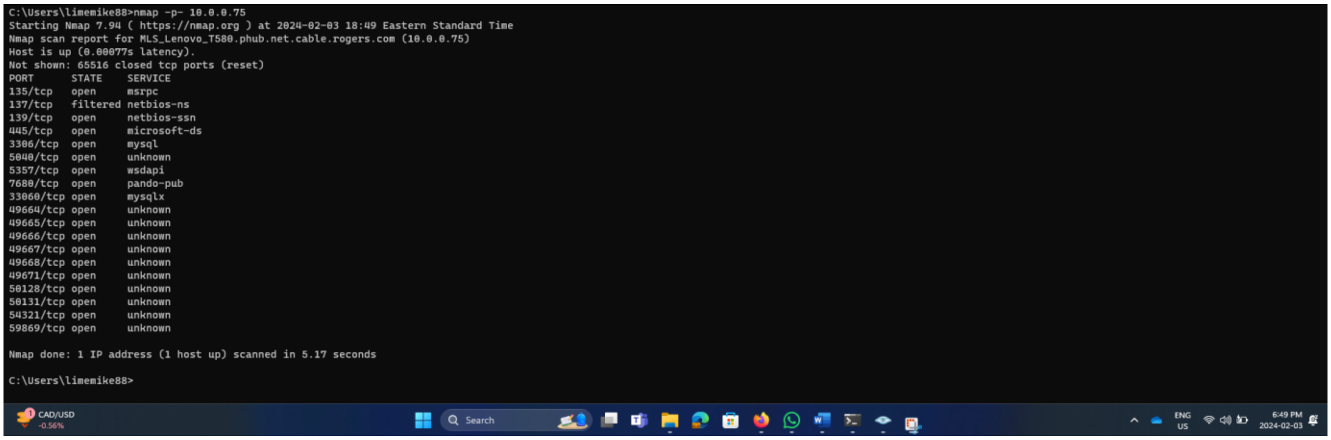
The Nmap scan using the -sS option, which performs a SYN scan, also known as a stealth scan. The break down the output are as follows:

- Starting Nmap 7.94: Indicates that the scan has been initiated using Nmap version 7.94.
- Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75): The scan was conducted against a host with the hostname MLS_Lenovo_T580.phub.net.cable.rogers.com and IP address 10.0.0.75.
- Host is up (0.0010s latency): Nmap confirms that the host is responsive, with a very low latency (1 millisecond), suggesting that the host is on the same local network as the scanning machine or is very close in network terms.
- Not shown: 995 closed tcp ports (reset): Nmap tried to connect to 1,000 common TCP ports (which is the default) and found that 995 of them are closed. Nmap classifies ports as closed when it receives a TCP RST (reset) packet in response to a SYN packet.
- PORT / STATE / SERVICE:
  - 135/tcp open msrpc: The Microsoft Remote Procedure Call service is running on port 135, which allows processes to communicate with each other over the network.

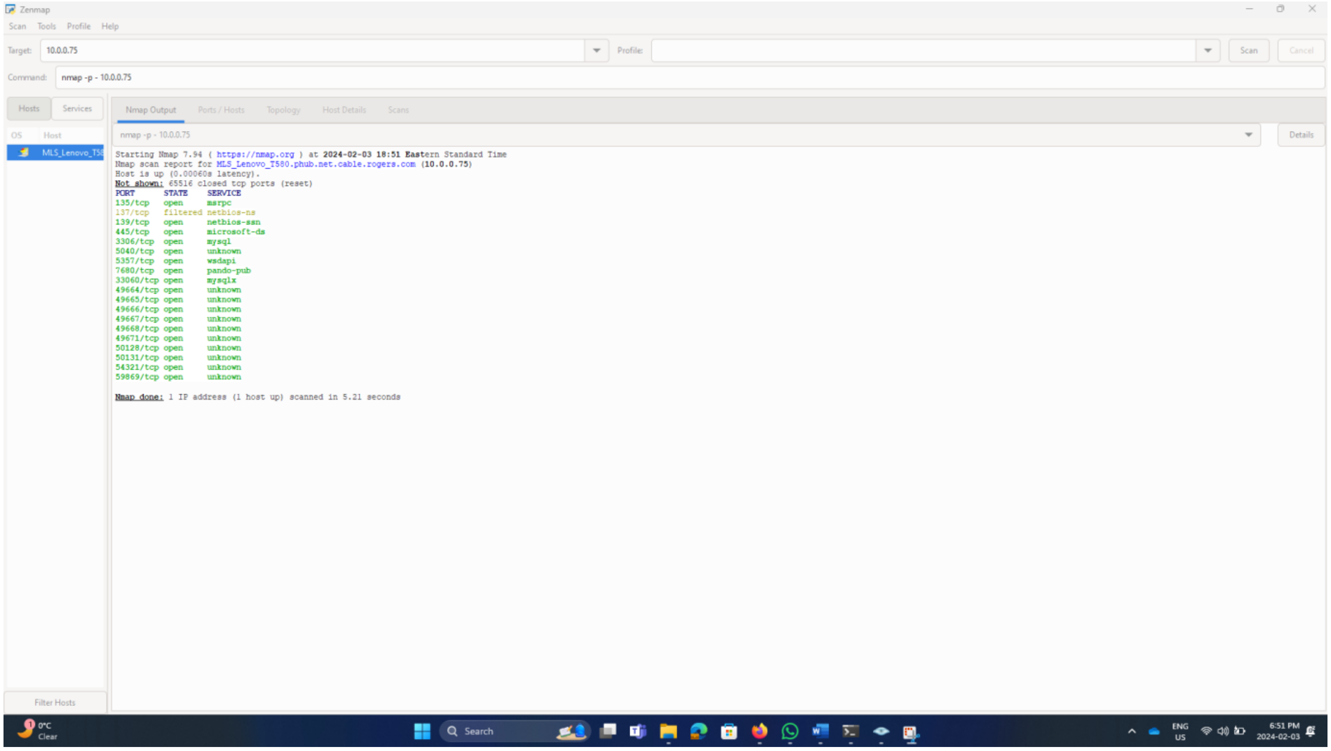
  - 139/tcp open netbios-ssn: Port 139 is open for the NetBIOS Session Service, used for file sharing and other network services on Windows machines.
  - 445/tcp open microsoft-ds: Port 445 is open, typically used by modern Windows machines for network file sharing with the Microsoft Directory Services.
  - 3306/tcp open mysql: The MySQL database service is accessible on port 3306.
  - 5357/tcp open wsdapi: The Web Services on Devices API (WSDAPI) service is listening on port 5357, which supports the discovery of devices on a network.
- Nmap done: The scan summary notes that the entire process scanned one IP address and took 0.38 seconds to complete. This quick scan time is typical for a SYN scan, as it only sends SYN packets without establishing a full TCP connection, which is a faster and less intrusive method of scanning.

The results indicate a standard setup for a Windows machine, with network services for RPC, NetBIOS, and SMB file sharing open, as well as a MySQL database service and a web service discovery API. The SYN scan is designed to be quick and stealthy, and it's often used to map out open ports on a networked device without establishing a full connection, which can sometimes go undetected by simple intrusion detection systems. However, the stealth benefits of a SYN scan can be less effective against modern security systems that are designed to detect such scans.

Performing nmap scan using "-p-" function in command prompt and Zenmap Gui:



```
C:\Users\limemike88>nmap -p- 10.0.0.75
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 18:49 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00077s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
3306/tcp  open     mysql
5040/tcp  open     unknown
5357/tcp  open     wsdapi
7680/tcp  open     pando-pub
33060/tcp open     mysqlx
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49671/tcp open     unknown
50128/tcp open     unknown
50131/tcp open     unknown
54321/tcp open     unknown
59869/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds

C:\Users\limemike88>
```



Target: 10.0.0.75

Command: nmap -p - 10.0.0.75

```
nmap -p - 10.0.0.75
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 18:51 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00060s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
3306/tcp  open     mysql
5040/tcp  open     unknown
5357/tcp  open     wsdapi
7680/tcp  open     pando-pub
33060/tcp open     mysqlx
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49671/tcp open     unknown
50128/tcp open     unknown
50131/tcp open     unknown
54321/tcp open     unknown
59869/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds
```

Explanation:

When running an Nmap scan using the -p- function, Nmap will scan the ports on the target system. The output will generally include the following information:

Ports: The specific TCP or UDP port number that was scanned.

State: The state of the scanned ports:

- Open: The port is accepting connections.
- Closed: The port is accessible but there is no application listening on it.
- Filtered: Nmap is unable to determine whether the port is open or closed because packet filtering prevents its probes from reaching the port.
- Unfiltered: The port is accessible, but Nmap cannot determine if it is open or closed.
- Open|Filtered: Nmap cannot determine whether the port is open or filtered.
- Closed|Filtered: This state is used when Nmap is unable to determine whether a port is closed or filtered.

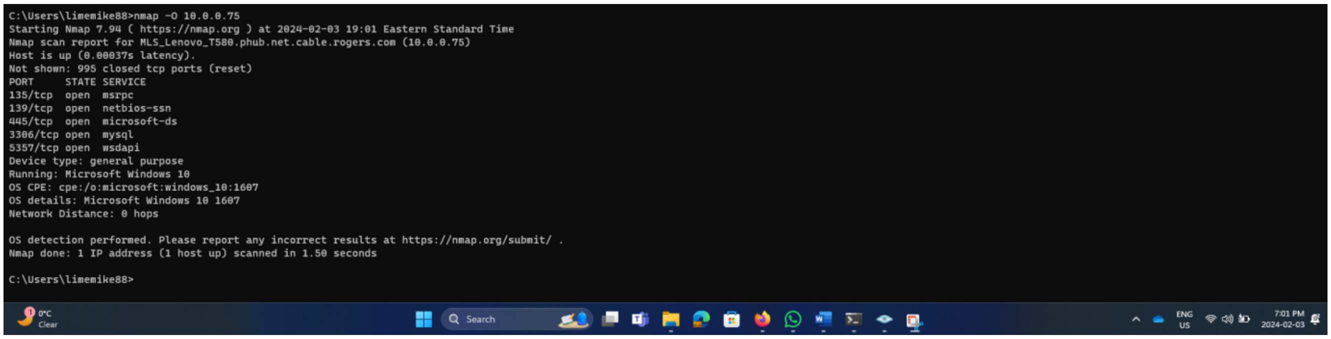
Service: The service that is typically associated with that port (for example, HTTP for port 80 and HTTPS for port 443).

Color-coding:

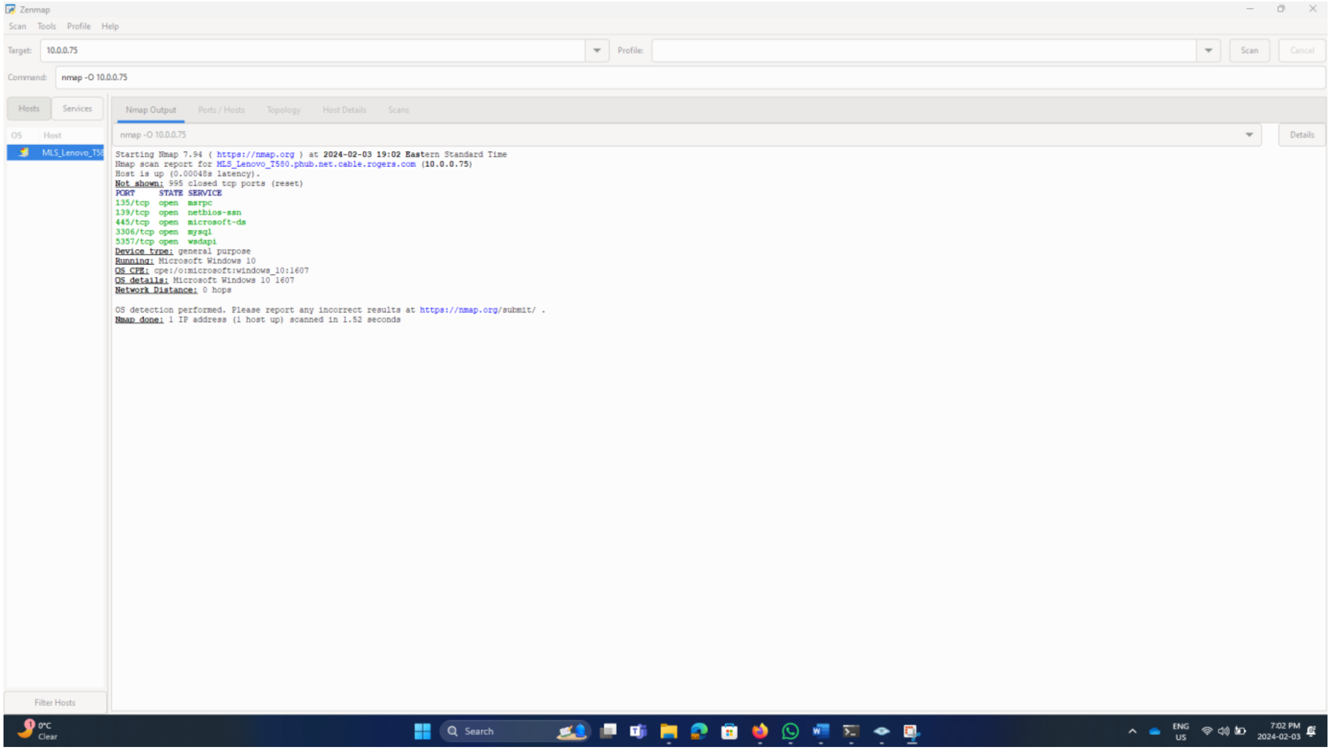
- Green might indicate an open port.
- Blue could signify a closed port.
- Red may represent a filtered port.

Lastly, the end of the scan summary will give a count of how many IP addresses were scanned, how many are up, and the total time the scan took.

Performing nmap scan using "-O" function in command prompt and Zenmap Gui:



```
C:\Users\limemike88>nmap -O 10.0.0.75
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:01 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00037s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds

C:\Users\limemike88>
```



```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:02 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00048s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

Explanation:

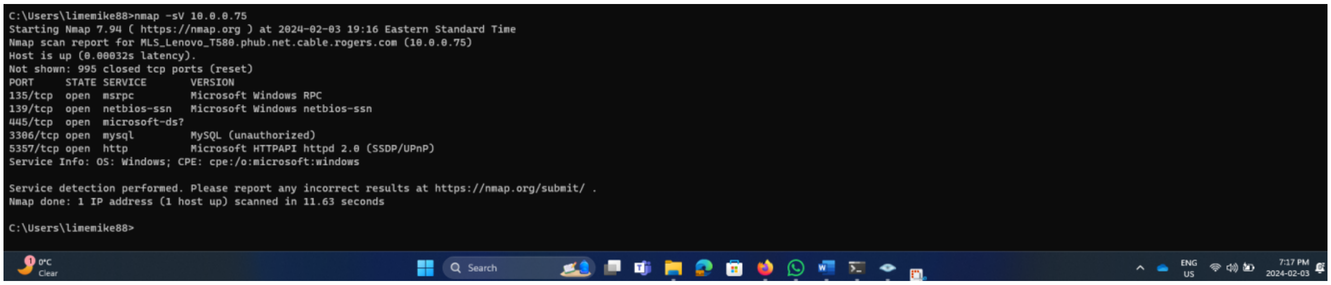
Nmap scan using the -O option, which attempts to identify the operating system of the target machine. Here's a breakdown of the results:

- Starting Nmap 7.94: This indicates the version of Nmap being used is 7.94, and the scan started at the given timestamp.
- Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75): This line identifies the target of the scan by its hostname and IP address.
- Host is up (0.00048s latency): Nmap has determined that the host is online, and the response latency is approximately 0.48 milliseconds, which is quite fast and typically indicative of a host on the same local network as the scanning machine.
- Not shown: 995 closed tcp ports (reset): Nmap found that 995 TCP ports are closed. Closed ports respond to Nmap's probes but no application is listening on them.
- PORT / STATE / SERVICE:
  - 135/tcp open msrpc: Port 135 is open and running the Microsoft RPC service.
  - 139/tcp open netbios-ssn: Port 139 is open for NetBIOS Session Service.

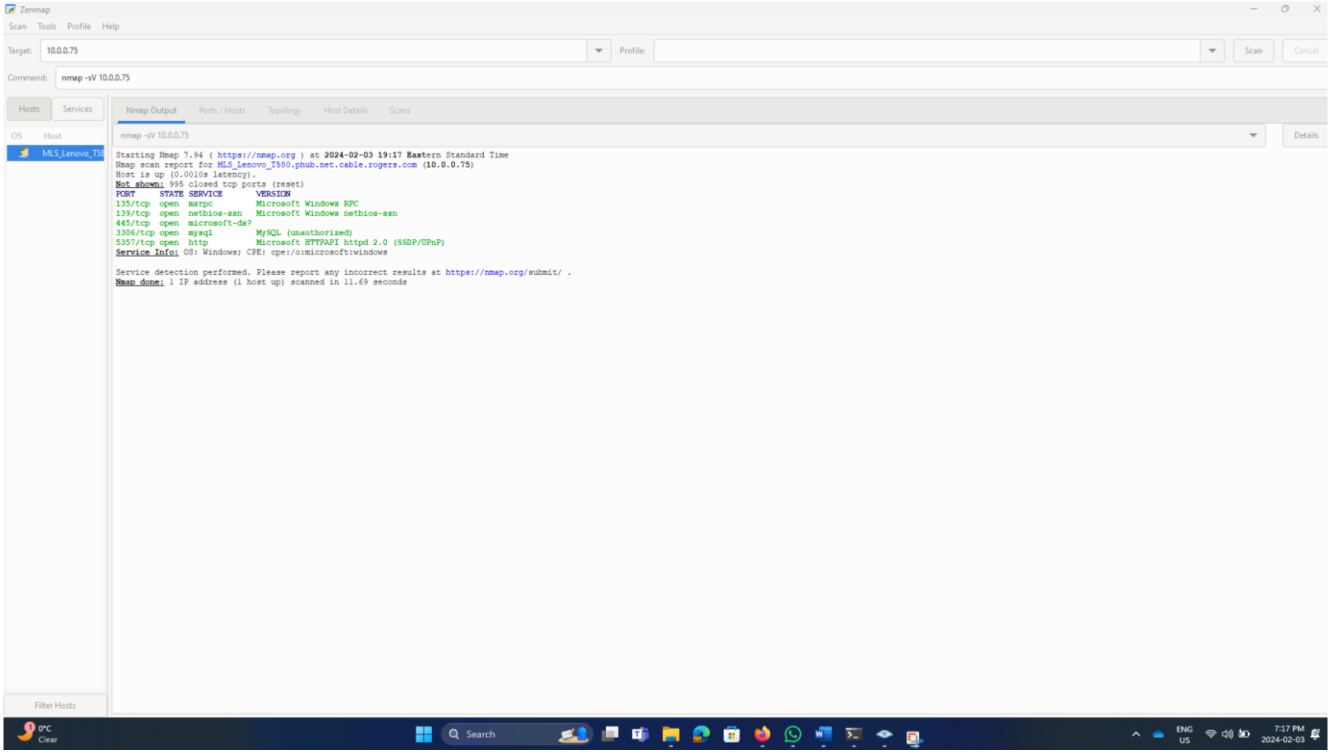
    - 445/tcp open microsoft-ds: Port 445 is open for Microsoft Directory Services, often used for file sharing in Windows.
    - 3306/tcp open mysql: Port 3306 is open, typically used by MySQL database server.
    - 5357/tcp open wsdapi: Port 5357 is open for Windows Web Services API.
- Device type: It's identified as a general-purpose device.
- Running: The scan has identified the device as running Microsoft Windows 10.
- OS CPE: The Common Platform Enumeration (CPE) for the identified OS is cpe:/o:microsoft:windows_10:1607. This means it has recognized the OS as Windows 10, version 1607.
- OS details: It gives more details about the operating system, confirming that it is Microsoft Windows 10 version 1607.
- Network Distance: 0 hops away, which means the host is on the same local network as the scanner, without any intermediate devices like routers.
- OS detection performed: This is a standard line indicating that OS detection was attempted, and the user is invited to report any incorrect results to Nmap for improving the tool's accuracy.

Overall, the scan has determined that the host is a Windows 10 machine with several typical Windows services running and open on the network. Also, the low network distance suggests this is likely an internal scan within a local network. Further, the host is running services that are commonly found on Windows machines, which can include RPC and NetBIOS services for various network operations and inter-process communication, a directory service for network file sharing, a MySQL service indicating a database server is running on the machine, and a Web Services API for service publication and discovery.

Performing nmap scan using "-sV" function in command prompt and Zenmap Gui:



```
C:\Users\limemike88>nmap -sV 10.0.0.75
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:16 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00032s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.63 seconds

C:\Users\limemike88>
```



```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:17 Eastern Standard Time
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.0010s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.69 seconds
```

Explanation:

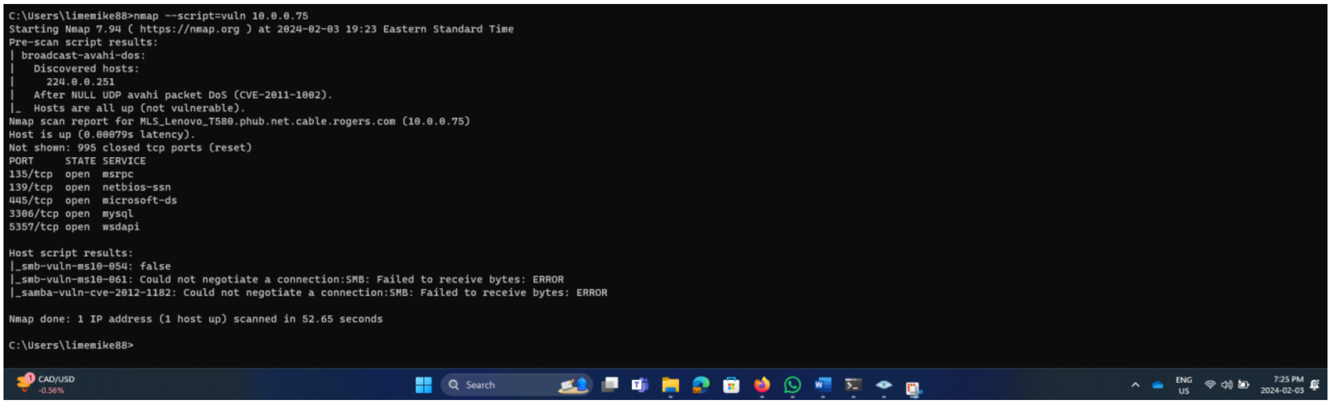
This Nmap scan output provides additional details compared to the previous one, especially regarding the services running on the open ports. The detailed explanation are as follows:

- Starting Nmap 7.94: The version of Nmap used for this scan is 7.94.
- Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75): The scan was conducted against the host with the specified hostname and IP address.
- Host is up (0.0010s latency): The target machine is online, and the latency of the response is 1 millisecond, indicating that the host is likely on the same local network.
- Not shown: 995 closed tcp ports (reset): There are 995 TCP ports that responded with a reset and are considered closed because no application is listening on them.
- PORT / STATE / SERVICE / VERSION:
  - 135/tcp open msrpc Microsoft Windows RPC: Port 135 is open and is running the Microsoft Windows Remote Procedure Call service, which enables different software components to communicate with each other.
  - 139/tcp open netbios-ssn Microsoft Windows netbios-ssn: Port 139 is open for NetBIOS Session Service, which allows applications on different computers to communicate over a local area network.
  - 445/tcp open microsoft-ds?: Port 445 is open for Microsoft Directory Services; the question mark indicates that the service version couldn't be fully confirmed.
  - 3306/tcp open mysql MySQL (unauthorized): Port 3306 is open, and there's a MySQL database service running. The "unauthorized" status suggests that the Nmap scan was not able to authenticate to the MySQL service (which is normal and expected unless supplied credentials).
  - 5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP): Port 5357 is open, running a web server using Microsoft's HTTPAPI version 2.0, typically used for SSDP (Simple Service Discovery Protocol) or UPnP (Universal Plug and Play) services.

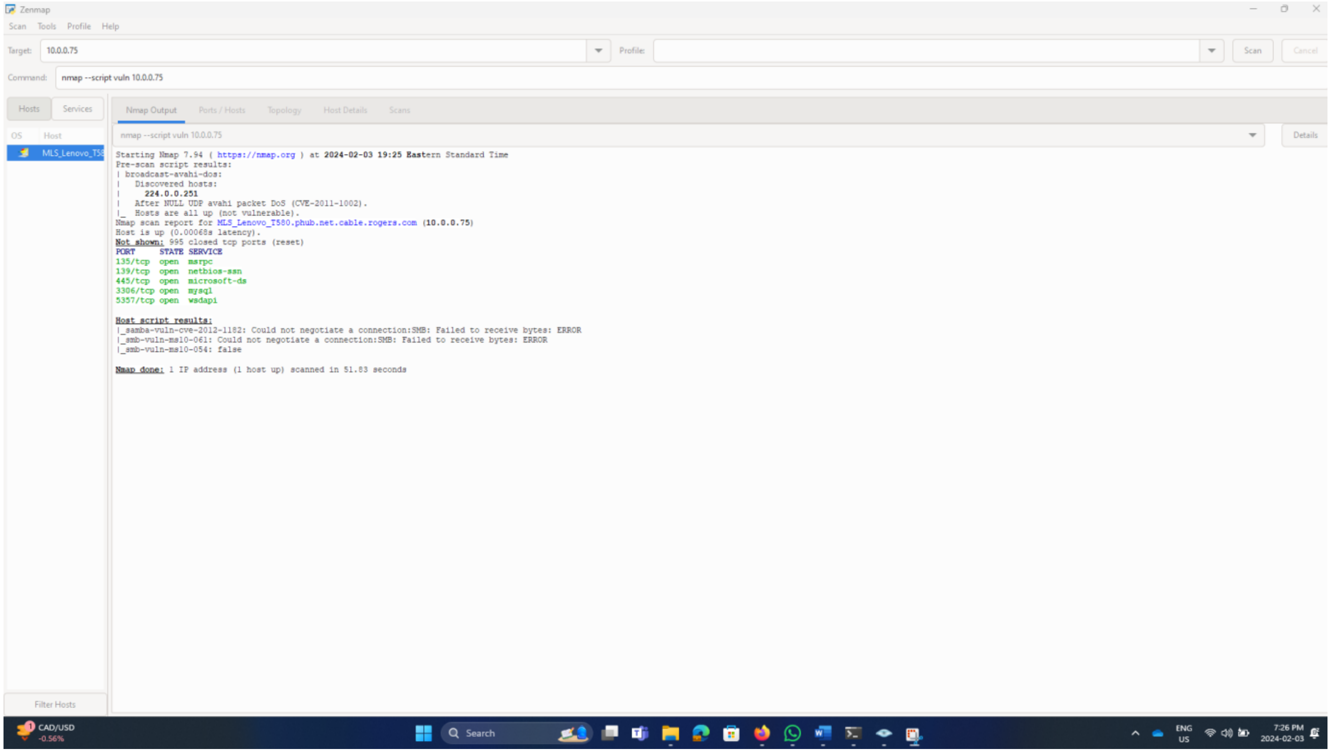
- Service Info: This line provides information about the operating system and the CPE (Common Platform Enumeration) for the detected services, indicating that the services are running on a Windows operating system.
- Service detection performed: This indicates that Nmap has attempted to determine the version of the services running on the open ports. It's a deeper level of scanning that probes services to identify their versions.
- Nmap done: The summary shows that the scan was completed on 1 IP address, and the target host was up and responsive during the scan, which took 11.69 seconds in total.

The services identified are typical for a Windows machine and suggest a system that is likely used for file sharing (given the SMB-related ports) and could be hosting or connected to a database (due to the open MySQL port). The HTTP service on port 5357 suggests that the system may be exposing some sort of web service or API, possibly for network device management or discovery.

Performing nmap scan using "-sS" function in command prompt and Zenmap Gui:



```
C:\Users\limemike88>nmap --script=vuln 10.0.0.75
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:23 Eastern Standard Time
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00079s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 52.65 seconds

C:\Users\limemike88>
```



Target: 10.0.0.75

Command: nmap --script vuln 10.0.0.75

```
nmap --script vuln 10.0.0.75

Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:25 Eastern Standard Time
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for MLS_Lenovo_T580.phub.net.cable.rogers.com (10.0.0.75)
Host is up (0.00068s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 51.83 seconds
```

Explanation:
The above Nmap output using the --script=vuln to detect vulnerability includes the results of both pre-scan and host scripts that check for specific vulnerabilities, in addition to the standard port scan results. The breakdown of the information are as follows:

Pre-scan Script Results:

- broadcast-avahi-dos: This script tests for a Denial-of-Service vulnerability in the Avahi service (CVE-2011-1002). The script found the multicast address 224.0.0.251, which is typically used by mDNS services like Avahi for service discovery on a local network.
- After attempting the exploit with a NULL UDP packet, the script reports that all discovered hosts are up and not vulnerable to this specific DoS attack.

Nmap Scan Report:

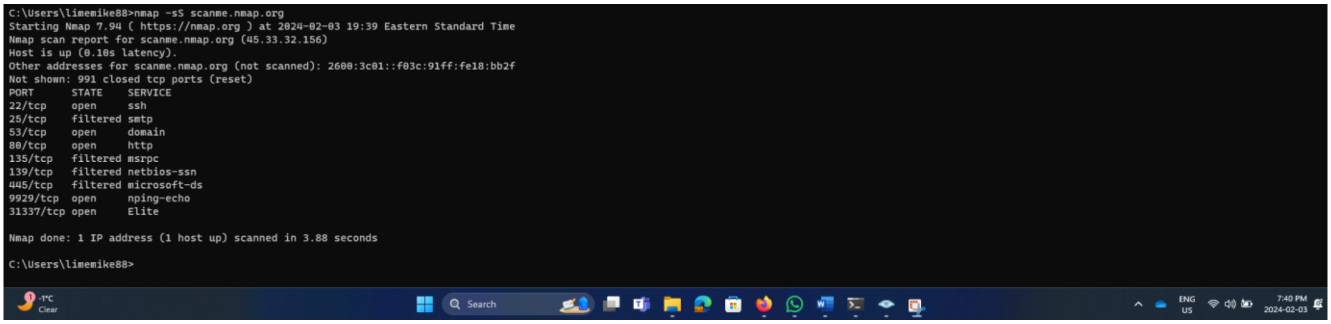
- The host MLS_Lenovo_T580.phub.net.cable.rogers.com with IP 10.0.0.75 is up with a latency of 0.00068 seconds.
- 995 TCP ports are closed, and the remaining ports listed are open.
- The open ports are the same as those in the previous scans, indicating services for RPC (135/tcp), NetBIOS (139/tcp), Microsoft Directory Services (445/tcp), MySQL (3306/tcp), and Web Services on Devices API (5357/tcp).

Host Script Results:

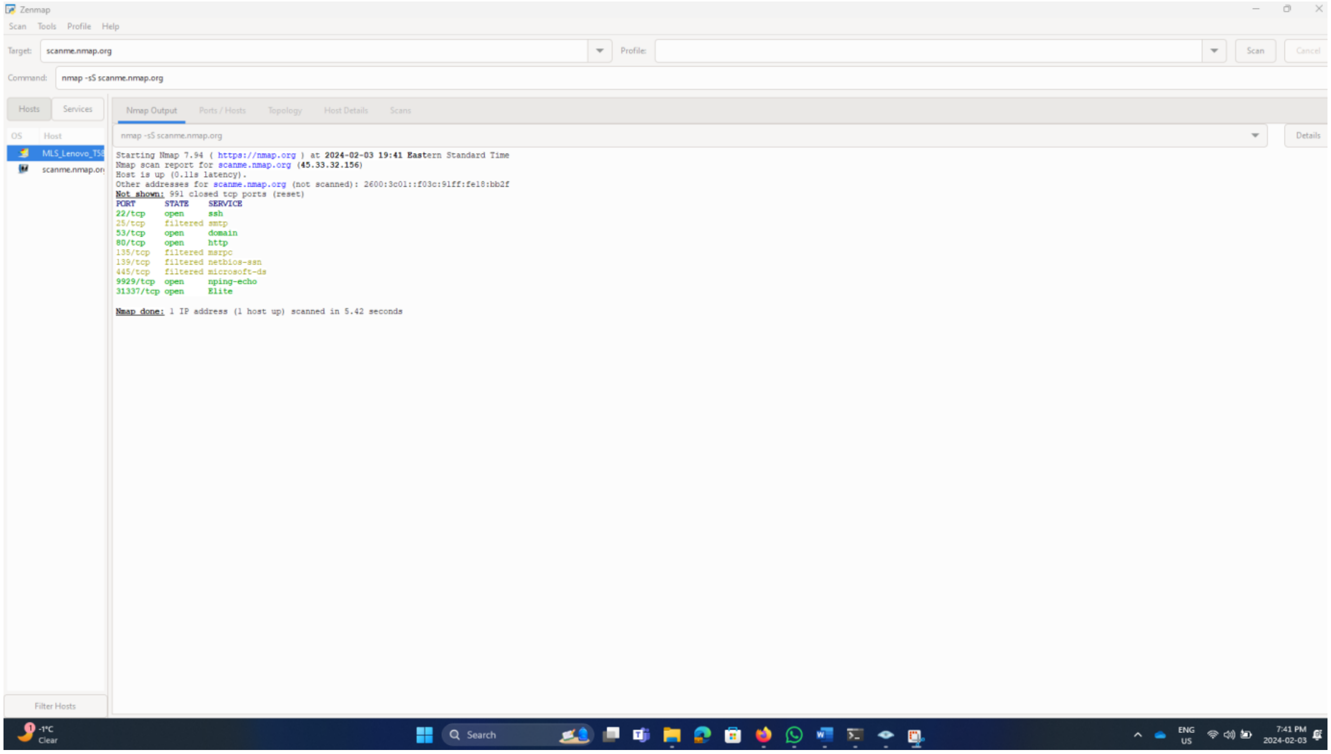
- samba-vuln-cve-2012-1182: This script checks for a vulnerability in Samba (CVE-2012-1182), which could allow remote code execution. The script could not negotiate a connection, which usually means that the service is not running Samba or is not vulnerable.
- smb-vuln-ms10-061: This script checks for a vulnerability described in MS10-061, which could be exploited to run arbitrary code via a crafted print request. Again, it could not negotiate a connection, indicating the host is not vulnerable or not running the vulnerable service.
- smb-vuln-ms10-054: This script checks for a vulnerability described in MS10-054 that could allow remote code execution if an attacker sent a specially crafted SMB packet to a computer that is running the Server service. The script returned false, indicating the host is not vulnerable to this specific vulnerability.

Overall, this Nmap scan suggests that the host is a Windows machine with common services running and is not vulnerable to the specific vulnerabilities checked by the Nmap scripts. It's important to note that a negative result from these scripts does not guarantee the system is secure; it only indicates that these vulnerabilities are not present.

Performing nmap scan using "-sS" function scanme.nmap.org site:



```
C:\Users\limemike88>nmap -sS scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:39 Eastern Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.10s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
53/tcp    open     domain
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 3.88 seconds

C:\Users\limemike88>
```



Target: scanme.nmap.org

Command: nmap -sS scanme.nmap.org

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-03 19:41 Eastern Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
53/tcp    open     domain
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 5.42 seconds
```

Explanation:

The outputs provided are from an Nmap SYN scan (-sS) targeting scanme.nmap.org. The detailed breakdown of the results are as follows:

- Starting Nmap 7.94: The scan was conducted using Nmap version 7.94.
- Nmap scan report for scanme.nmap.org (45.33.32.156): The scan is reporting on the host with the domain name scanme.nmap.org, which resolves to the IPv4 address 45.33.32.156.
- Host is up (0.11s latency): The target is online and responsive with a latency of 110 milliseconds.
- Other addresses for scanme.nmap.org (not scanned): This indicates that the domain scanme.nmap.org also resolves to an IPv6 address, which was not scanned in this command.
- Not shown: 991 closed tcp ports (reset): Nmap has determined that 991 of the 1,000 most common TCP ports are closed because they responded with a TCP reset packet.
- PORT / STATE / SERVICE:
  - 22/tcp open ssh: The Secure Shell (SSH) service is running on port 22, which is typically used for secure remote administration.

  - 25/tcp filtered smtp: The Simple Mail Transfer Protocol (SMTP) service is typically found on port 25. The "filtered" state indicates that Nmap could not determine whether the port is open because the packets are being dropped, possibly by a firewall.
  - 53/tcp open domain: The Domain Name System (DNS) service is running on port 53, which is used for resolving domain names to IP addresses.
  - 80/tcp open http: The Hypertext Transfer Protocol (HTTP) service is running on port 80, indicating a web server is operational.
  - 135/tcp filtered msrpc: The Microsoft Remote Procedure Call (MSRPC) service typically runs on port 135. It is marked as "filtered", suggesting that a firewall or filter is blocking Nmap's probes.
  - 139/tcp filtered netbios-ssn: The NetBIOS Session Service is generally found on port 139 and is also marked as "filtered".
  - 445/tcp filtered microsoft-ds: Port 445 is used by Windows machines for network file sharing with the Microsoft Directory Service, also "filtered".
  - 9929/tcp open nping-echo: Nping Echo service is running on port 9929. This is an Nmap's own service used for response analysis and is indicative of an Nmap test server.
  - 31337/tcp open Elite: This port is historically associated with backdoor trojans and is often used in examples and tests. Its presence here, along with nping-echo, suggests that this server is used for Nmap scanning exercises.
- Nmap done: The scan summary indicates that the entire process scanned one IP address, took 5.42 seconds to complete, and the target host was up and responsive during the scan.

This output is characteristic of scanme.nmap.org, which is a host provided by the Nmap project for users to test Nmap legally. The open services reflect common services one might find on a server, along with some services (like nping-echo and port 31337) that are there for testing and educational purposes. The "filtered" ports suggest that a firewall is present and is configured to drop packets directed to those ports, making it impossible for Nmap to determine whether they are open or closed without further analysis or different scanning techniques.

Conclusion:

This project underscores Nmap’s value as an essential tool for network security analysis and proactive threat detection. Through port scanning, service identification, OS fingerprinting, and vulnerability detection, I demonstrated skills in assessing network security risks and implementing actionable solutions to protect critical infrastructure. This practical experience reflects my ability to conduct real-world network assessments, ensure compliance, and maintain secure IT environments.